BACKUP/RECOVERY SYSTEM AND
METHODS FOR PROTECTING A COMPUTER SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a backup/recovery
5   technique for a computer system, and more particularly to a
method for protecting a computer system with a
backup/recovery system.

2. Description of Prior Art

10   The protection for the computer system is an important
issue for a computer user at present. Chain mails for the
spread of virus by way of Internet are increasingly
overabundance in virtue of vigorous development of network.
Modern people get used to E-mail (electronic mail) as the
15   connecting interface between human beings. Afterwards, they
often receive greetings and messages send from others, as
well as the annoying spams and impossible to guard against
viruses smuggled by concealing in between the mails.

Computer viruses are buried or hidden in another
20   program. Once the program is executed, the virus is
activated and attaches itself to other programs in the
system. Nowadays, viruses are frequently spread by the
smuggling with files in a predetermined form, such as *.EXE,
*.DOC, and *.ZIP form attached to the e-mails. When the user
25   is ignorant of what happened and operates the attached
files, the computer will be affected by poison. Viruses will
send themselves to the entire name list of the users' record
of communication. If the users relax their vigilance and
operate the virus-smuggled files, there will be a chain-
30   infected reaction that causes the disaster worldwide.

Moreover, for the PC (personal computer) users, they will risk interconnecting of computers into networks. In case of the viruses infected their computers, viruses usually destroy the files throughout the user's disks and all
5 computer files may be deleted that lose the essential data in the twinkling of an eye and cause the computer system operates out of order. If operating system files have been infected and destroyed, Windows cannot be rebooted. The more serious effect such is that the computer system needs to be
10 re-setup. Hence, there is a need for eliminating viruses from computers and networks.

Conventionally, a used backup/recovery software, although having the backup/recovery function, it is capable of executing the backup program for backing up data, also of
15 executing the recovery program for restoring the data to the HD, in order to protect HD return to the normal state. Nevertheless, not only the HD is not protected thoroughly, but also the backup/recovery action wastes the user a long time.

20 For instance, a prior Ghost backup/recovery software researched by Symantec Corporation in U.S.A., its backup/recovery action needs the network administrator to operate the operating system (OS) before he/she operate the Ghost backup/recovery program manually. Ghost backup program
25 backs up data stored in the selected hard disk/partition to a file totally, and Ghost recovery program restores the data from the file to the selected hard disk/partition. It is a single task procedure to create a backup with Ghost that all of other tasks should stop ahead, and it spends a period of
30 time about 8 minutes/ Gb, in general. Besides, owing to the Ghost software backs up all the valid data stored in the hard disk, the space of the hard disk for backing up data occupied by the Ghost software is extremely large. The data provided

that being used in the file system of the operating system (OS) will be backed up the belonged area to the file absolutely, nevertheless whether it has been changed or not afterwards, causing a great amount of space being occupied.

5   Further, another prior backup/recovery software, Goback, designed by adaptec Corporation in U.S.A., it operates the recovery action program without the need of operating the operating system (OS) in advance. The system is indicated to initiate the recovery operation, and then the Goback software
10   recoveries the hard disk to selected status. When the computer system is destroyed, the action of restoring disk files also needs the network administrator to operate the recovery program manually.

Obviously, when the computer system is surfing the web
15   or receiving electronic mail accesses by multiple users, the virus will easily infected the user's disks. The virus will further break out that cause the computer system damaged unexpectedly or more serious effects such as the system cannot be booted. Nevertheless, the used backup/recovery
20   software is unable to distinguish the possible danger of receiving data from Internet effectively, not to mention the fact that it is incapable of backing up data immediately.

Conversely, various prior art devices have been proposed for the detection of virus intrusions on the computer system.
25   The InterScan VirusWall produced by Trend Micro Corporation, it provides Internet gateway protection against viruses and malicious code. The detection is for all SMTP, HTTP, and FTP Internet traffic at the gateway and blocks malicious mobile code at the gateway. It can be configured to respond to virus
30   detection and security violation incidents in three ways, such as alerts the system administrator, just deletes the infected file or permits the user to download the file under

certain controlled conditions, optionally isolates the infected file for later treatment.

The previous anti-virus software may provide Internet real-time virus detection during surfing the web and blockage
5 of viruses included with electronic mails, however, the backup/recovery technique is not available. This results in a harm of the hard disk for a computer system. As described above, the anti-virus software cannot backs up and retrieves data. Hence, in case of contingency, the computer system is
10 damaged, the disks cannot return to normal immediately. The demand of real-time backup/recovery for the user cannot be satisfied.

Accordingly, because of the presently anti-virus software contains without backup/recovery function and other
15 backup/recovery software products cannot recognize the possible danger of receiving data from Internet to protect the computer system as well. There is a need in the art to provide a backup/recovery software for protecting a computer system.

20 The present invention overcomes the limitations and shortcomings of the prior art with systems and methods for protecting a computer system with files backup to the hard disk automatically prior to downloading data to the end-users. It will be appreciated that the system and method of
25 the present invention may provide computer system protection from viruses introduced by data downloaded from the largely unregulated network.

SUMMARY OF THE INVENTION
30 Accordingly, an object of the present invention is to provide a backup/recovery system and methods, which can be used in a computer system to securely backs up and reliably retrieves data. The improvement is remarkable for the data

storage means while its data is under whole automatic protection from viruses.

To achieve the above and other objects, this invention applies a detecting module in the backup/recovery system to

5 monitor a predetermined message to be downloaded to the computer system. When a predetermined message is received, the detecting module determines whether there is a predetermined harmful data contained in the predetermined message. If there is a predetermined harmful data contained

10 therein, backup/recovery system backs up data automatically prior to downloading such data, so as to protect the computer system.

One aspect of the present invention involves a backup/recovery system for detecting and backing up data

15 immediately. The backup/recovery system is installed in a computer system. The computer system includes an application layer, which coupled to an interface. The backup/recovery system comprises a detecting module, located within the computer system, for monitoring a predetermined message. The

20 detecting module retrieves the predetermined message, in order to determine whether there is a predetermined harmful data contained therein for judging the backup/recovery system to backup data or not. The interface implements a predetermined procedure thereafter and the application layer

25 involves reading the predetermined message.

Another aspect of the present invention involves a method for protecting a computer system. The method comprises three steps. First, the backup/recovery system retrieves a predetermined message to be downloaded to the

30 computer system. Secondly, upon retrieval of a predetermined message to be downloaded, determines whether a predetermined harmful data is contained in the predetermined message. If the is predetermined harmful data is contained, the data

stored in the computer system is backed up eventually, in order to enable the computer system to return the data storage means to a preceding status while the viruses infect the storage means.

5   Further aspect of the present invention involves a method for protecting a computer system with a backup/recovery system. The computer system includes an application layer coupled to an interface. The method comprises several steps. First, the backup/recovery system

10   installs in the computer system. The backup/recovery system comprises a detecting module for monitoring a predetermined message located within the computer system. Secondly, the detecting module retrieves the predetermined message to be downloaded to the computer system. Upon retrieval of a

15   predetermined message to be downloaded, determines whether a predetermined harmful data is contained in the predetermined message. If the is predetermined harmful data is contained, the data stored in the computer system is backed up. Then, the interface implements a predetermined procedure.

20   Eventually, the application layer is indicated to read the predetermined message.

In the preferred embodiment of the invention, the backup/recovery system is coupled to a network device. The network device is coupled to at least one client device by a

25   communications link. The network device is coupled to a server device. The server device is capable of controlling the client device's backup/recovery conduct remotely and immediately. The network device comprises a network means, comprising one or more of the group consisting of a LAN,

30   WAN, Internet, Intranet, Extranet and wireless network. The network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP. The predetermined

harmful data comprises a file in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP form.

It is to be understood that both the foregoing general
5 description and the following detailed description are exemplary, and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

10 The above-mentioned objects and other objects and features of this invention and manner of attaining them will become apparent, and the invention itself will be understood by reference to the following description of the preferred embodiments of the invention taken in conjunction with the
15 accompanying drawings, wherein:

FIG. 1 illustrates parts of a computer system with a backup/recovery system as per an embodiment of the invention;

FIG. 2 illustrates a flowchart of the computer system
20 with a backup/recovery system as per an embodiment of the invention;   and

FIG. 3 illustrates a schematic diagram of the hard disk return to a state of the preceding state for protecting the computer system as per an embodiment of the invention.

25

DESCRIPTION OF THE PREFERRED EMBODIMENT

Reference will now be made in detail to the present preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever
30 possible, the same reference numbers are used in the drawings and the description to refer to the same or like parts.

The present invention contemplates a backup/recovery system to provide protection for the computer system by way of a detecting module of the backup/recovery system. The real time backup/recovery system adopts a technique for

5 detecting network data to be downloaded to the computer system, such as data retrieved from an Internet content server in response to a browser request, which can automatically backup any file alteration to the hard disk. Here is referred to the data to be downloaded, it being

10 understood that the invention is capable of use in various other combinations and environments and is capable of changes or modifications within the scope of the inventive concepts as expressed hereunder.

The preferred embodiment of the present invention

15 provides a backup/recovery system installed in the computer system. The computer system comprises at least an application layer, which coupled to an interface. The application layer is for operating a predetermined application program. The backup/recovery system comprises a

20 detecting module, located within the computer system, for monitoring a predetermined message.

When the predetermined message is received, the detecting module determines whether there is a predetermined harmful data contained in the predetermined message. If

25 there is a predetermined harmful data contained therein, the backup/recovery system backs up data, and the interface implements a predetermined procedure thereafter, so that application layer can read the predetermined message.

With reference to FIG. 1, according to an embodiment of

30 the present invention a backup/recovery system may recognize the possible danger of receiving data from network effectively, and may create a restoration point immediately to backup data as well.

The computer system includes an application layer 2 and a driver layer 4. The application layer 2 is for operating a predetermined application program, and the driver layer 4 is for operating a predetermined driver program. The application layer 2 is coupled to an interface, which installs the corresponding protocol module stored therein at the time of initiating.

The application layer 2 is a layer for operating the application program. The application layer 2 has an Internet Application 20. All of the network application programs, such as Internet Explorer, Outlook Express, FTP utilities and TELNET utilities, are operated at the application layer 2.

The driver layer 4 is a layer for operating the driver program. All of the network driver programs are operated at the driver layer 4. The driver layer 4 provides the network access service for the application program, and accesses LAN (local area network) and distributed system (Internet) 6 through the network interface card or other network system. The driver layer 4 has a network driver 40.

The backup/recovery system may couple to a network device. The network device is coupled to at least one client device by a communications link. The network device is coupled to a server device. The server device is capable of controlling the client device's backup/recovery conduct remotely and immediately. The network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network. The network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

The backup/recovery system comprises a detecting module 42, a network monitor driver. The detecting module 42 may get in the application layer 2 or the driver layer 4 upon the backup/recovery system installed in the computer system.

5 While in the preferred embodiment of the present invention, the detecting module 42 of the backup/recovery system gets in the driver layer 4 for monitoring a predetermined message to be downloaded to the computer system.

When the predetermined message is received, the

10 detecting module 42 retrieves the message. The predetermined message is coming from the behavior of downloading from the network or the receiving electronic mail via Outlook Express, comprising HTTP pages, E-mails, downloading files and so forth.

15 Furthermore, the detecting module 42 determines whether there is a predetermined harmful data contained in the predetermined message, in order to judge whether the backup/recovery system creates a restoration point to backup data. The predetermined harmful data includes the possible

20 harmful data, which comprises a file in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP form. Other types of files are included as well.

That is, the detecting module 42 will retrieve all

25 downloading data the application layer 2 call on the network and the receiving electronic mail via Outlook Express. The detecting module 42 monitors the data to be downloaded to the computer system. If there is a predetermined harmful data contained therein, the backup/recovery system may

30 create a restoration point immediately to backup data as well prior to downloading data to the end-users.

Thereafter, the detecting module 42 sends the predetermined message to the computer system. After the

interface implements a predetermined procedure, such as dealing with the protocol module and the uniform format handling for the received data, the application layer 2 is informed to read the predetermined message.

5   Thereupon, if the received data cause damage to the computer system, it is capable of returning the storage device to the preceding condition immediately.

Accordingly, the backup/recovery system as per the preferred embodiment of the present invention installed in the computer system may monitor all information from the network. Once it detects the downloading conduct or the electronic mail received by Outlook Express, it creates a restoration point immediately with the valid data.

The detecting module 42 monitors all information from the network entirely. Therefore, if viruses and malicious code smuggling with the downloading data or the receiving electronic mail that activated and caused the system crash, the system still can return to the normal state.

The present invention meditates a method for protecting a computer system. The method comprises three steps. First, the backup/recovery system retrieves a predetermined message to be downloaded to the computer system. Secondly, upon retrieval of a predetermined message to be downloaded, determines whether a predetermined harmful data is contained in the predetermined message. If the is predetermined harmful data is contained, the data stored in the computer system is backed up eventually, in order to enable the computer system to return the data storage means to a preceding status while the viruses infect the storage means.

In the preferred embodiment of the invention, the present invention contemplates a method for protecting a computer system with a backup/recovery system. The computer system includes an application layer coupled to an

interface. First, the backup/recovery system installs in the computer system. The backup/recovery system comprises a detecting module for monitoring a predetermined message located within the computer system. Secondly, the detecting

5 module retrieves the predetermined message to be downloaded to the computer system. Upon retrieval of a predetermined message to be downloaded, determines whether a predetermined harmful data is contained in the predetermined message. If the is predetermined harmful data is contained, the data

10 stored in the computer system is backed up. Then, the interface implements a predetermined procedure. Eventually, the application layer is indicated to read the predetermined message.

FIG. 2 illustrates a flowchart of the computer system

15 with a backup/recovery system as per an embodiment of the invention. First of all, Step S10 is to monitor the message to be downloaded to the computer system. Upon the message is arrived; the detecting module 42 retrieves the message and determines the message in advance.

20 Step S30, a second step, is to ascertain by the detecting module 42, whether the network message is downloaded to the computer system. The detecting module 42 analyzes the contents contained in the message and determines whether the message is the predetermined message

25 the users applied to be downloaded. If not, then goes to Step S90, and sends the message to the upper layer.

If yes, then goes to Step S50. The predetermined message is coming from the behavior of downloading from the network or the receiving electronic mail via Outlook

30 Express, comprising HTTP pages, E-mails, downloading files and so forth.

Step S50, a third step, is to determine further whether the message contains a predetermined harmful data by the

detecting module 42. For example, the possible harmful data may comprise a file in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP form. If not, such data like TXT, bitmap, then goes to Step

5 S90 either, and the detecting module 42 sends the message to the upper layer.

If yes, then goes to Step. S70. The backup/recovery system creates a restoration point automatically to backup data prior to downloading data to the computer system.

10 Step S90, a final step, is to send data by the detecting module 42. After the interface implements a predetermined procedure, such as dealing with the protocol module and the uniform format handling for the received data, the application layer 2 is informed to read the

15 predetermined message.

Hence, if the received data cause damage to the computer system, it is capable of returning the storage device to the preceding condition immediately.

The flow of creating a restoration point in Step S70 is

20 to scan the entire disk recognizing the valid data. Each restoration point contains the message of which data in the disk is valid data. While creating a new restoration point, the information of the valid data is stored therein.

Please be noted that the MSTCP protocol, which is

25 defined by the Microsoft, is communicated with the Http/Ftp/Pop3 application protocols through TDI (Transport Driver Interface) layer. In the preferred embodiment of the present invention, the detecting module 42 is. intercepting network data at TDI layer.

30 The Http/Ftp/Pop3 application protocol sends data to Internet through TdiSendEntry(), the entry function of TDI layer, and while Internet sends data back, MSTCP protocol produces an event. An event handler function set by

SetEventEntry()handles this event, TDI_EVENT_RECEIV. If we change the address of the function entry, the function entry of TdiSendEntry() and SetEventEntry(), then we can intercept the network data.

5   When we operate Outlook Express to receive mails, Outlook Express will send a request of receiving mails to the mail server on Internet. All data Outlook Express sent to Internet will pass through TDI layer, and the driver program of TDI layer will recognize the user is going to receive

10   mails, and the driver program revise the address entry of the event returning mails from the mail server on Internet.

      While the receiving mails send back, system will use event handler function of thedriver program. The event handler function handles the data contained in the mails. If

15   there are viruses or unsafe files founded in the mails, the driver program of TDI layer will inform the driver program of the backup/recovery system as per the preferred embodiment of the present invention of creating a new restoration point.

      In the preferred embodiment of the present invention,

20   the new restoration point is stored the information of the valid data. In the process of backing up data, the data demanded to backup is stored in the new restoration point.

      After that, the driver program sends the mail to Outlook Express. If the users read their mail that caused the disk

25   damage, then the user may return the disk to a state of the preceding state.

      With reference to FIG. 3, according to an embodiment of the present invention a backup/recovery system may return the disk to a state of the preceding state. The state A of the

30   hard disk in the computer system is in normal conditions. However, the detecting module 42 determines the predetermined message is contained a predetermined harmful data,   and the

backup/recovery system creates a new restoration point to backup data.

Right after that, the detecting module 42 sends the predetermined message to the computer system. The network interface implements a predetermined procedure thereafter and the application layer 2 involves reading the predetermined message. The user probably downloads a virus-infected program, UNKNOWN.EXE, but the user has no idea.

The predetermined message is with viruses, and the state B of the hard disk in the computer system is in abnormal conditions. Then, viruses are activated and damage the system, as shown in FIG. 3, the state C of the hard disk in the computer system is in destroying conditions.

Nevertheless, if there is an accident, the user can return the disk to a state of the preceding state with the backup/recovery system as per the preferred embodiment of the present invention. The computer system is easily infected viruses while the user downloads data or reads mails, but the hard disk is capable of returning the hard disk to a normal state due to the backup/recovery system in the preferred embodiment of the present invention backs up the valid data being changed stored in the hard disk prior to downloading data to the computer system. Consequently, the system and the programs will never be lost or destroyed.

While this invention has been particularly shown and described with reference to embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.